User Manual

Fingerprint Reader

All instructions in this user manual is for full functions. The actual functions are based on real fingerprint products.

Please review this user manual in detail before using Fingerprint product. Please keep this user manual for future reference

PC WINNER INTERNATIONAL INC

5F., No.1, Lane 21 Singhua Road Taoyuan City 330, Taiwan

Telephone:(03)362-6020 FAX:(03)362-5685

Table of Content

Table of Content **2**
Overview **3**
What is User Data File? **3**
System Requirements **4**
Instruction on Fingerprint Input **22**
Installing and Removing Applications **4**
Installing Application 4
Uninstall Application 11
Operating Instructions **14**
To Start Using 14
System Setting 14
Fingerprint Management 15
General Setting 16
Computer Protection Management 17
Password Bank Management 18
Application Protection Management 19
Backup 21
Restore 22
Password Bank 22
Set up Password Bank 22
Usages for Password Bank 22
File Protection 27
File Encryption 28
File Decryption 30
Editing Encrypted Files 31
Computer Protection 31
Login Computer 31
Locking Computer 32
Screen Saver 33
Application Protection 34
Search Protected Files 35
Hiding/Displaying icon on toolbar 36
FAQ **37**

Overview

First of all, thank you for choosing this Fingerprint Application Suite. People are growing increasingly dependent on computers, more and more important documents are stored in computers. As this trend continues to grow, “security” issue becomes more worrisome to us than ever before. Amount all file protection methods, “Fingerprint” stands out as the best method to fulfill your requirement for protecting files and computers. This product utilizes the uniqueness and convenient characteristics of fingerprint to help you properly protect your personal information environment.

Your important information will receive double protections – your fingerprint date and File Protection secret key that is produced based on the fingerprint. “File Protection secret key” is a 24 bit random number. After you have successfully installed the application and created fingerprint information, the system will automatically produce the sedret key. This key will be safely stored in user information file and be utilized by protection mechanism inside user information file to protect every file that needs protection.

Computer brings convenience into our lives, we hope this production will help you use computer with a peace of mind.

What is User Data File?

After you have successfully installed the application and created fingerprint information, this application will create “User Data File”. User Data File includes: your fingerprint data, File Protection secret key, configuration values for Password Bank, configuration values for Application Protection.

We strongly recommend you to back up current User Data File. This is due to the fact that every re-installation of this application, a new file encryption key and user data file will be created (please refer to “Installing and removing application” section of the manual). If you cannot restore previous user data file, it would not be possible to access previously protected files. Restore action will not replace the newly generated file encryption key. Instead, the new key and the old key will be both utilized. This means that restored user data file will have two keys so your files will be protected by two keys.

> Note
> The security mechanism of this application is based on your safe usage and protection of password. When your password is compromised, it is possible to lose files.

System Requirements

Hardware system requirement: PC, MAC and Notebook with USB port.

OS requirement: support Microsoft Windows XP, Windows 2000.

CPU: recommend PIII 700 and above.

RAM: 128MB and above

Browser: IE 5.0 and above

Video card: Support VGA, 800x600 resolution and above

Recommend 1024x768, Small Font, True Color.

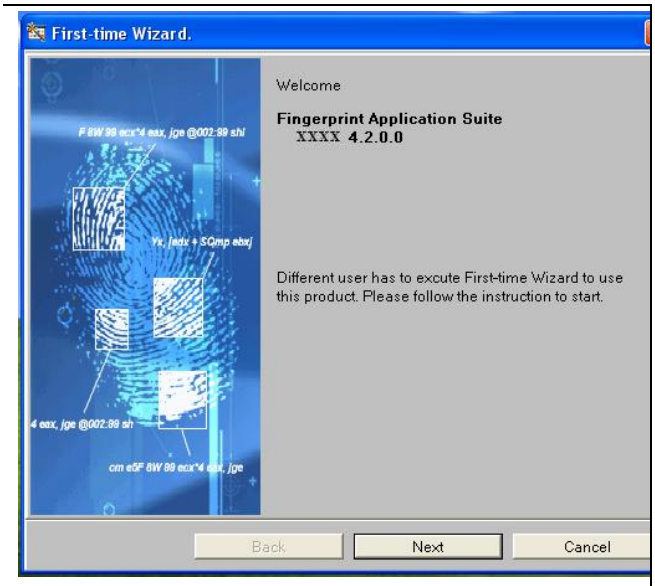
Installing and Removing Applications

Installing Application

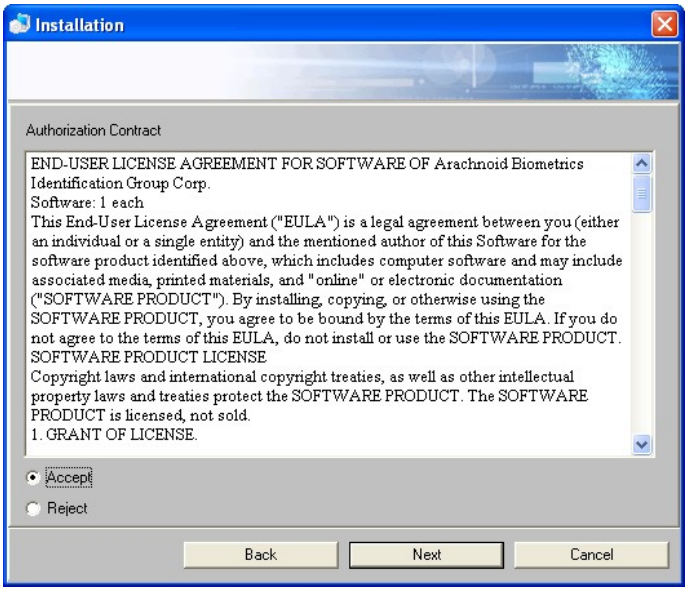
Please insert fingerprint device into USB port of the computer. To raise production security, please make sure your computer account password is not blank.

Operating procedures

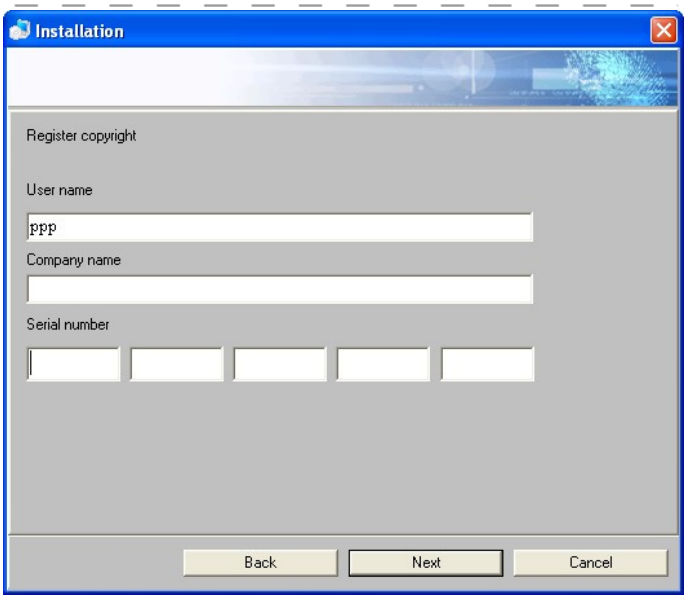
1. After inserting Fingerprint Application Suite CD into CD ROM, the installation program will start automatically (if it does not start automatically, please double click setup.exe located in the CD). To continue installation, please click “Next”, to cancel installation, please click “Cancel” to exit. (“XXXXX” in the figure represents product model number)



2. You have to select “Accept” before you can continue installation. After you have accepted license agreement, click “Next” to continue following steps.

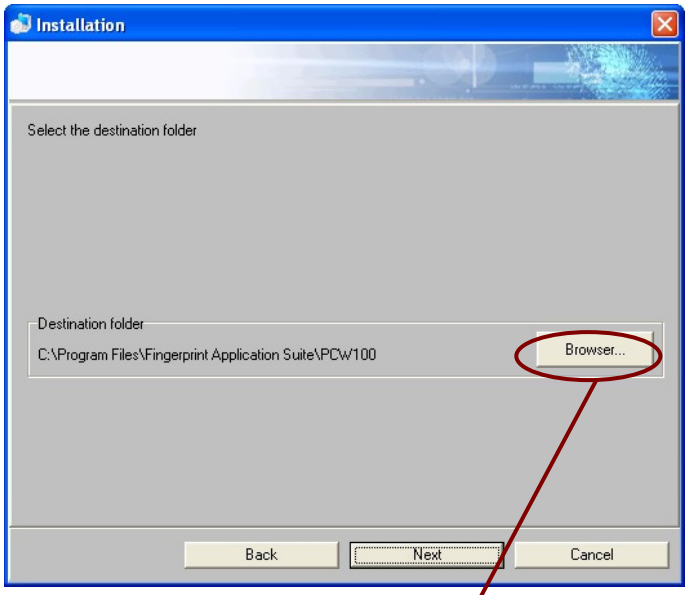

Installation
Authorization Contract
END-USER LICENSE AGREEMENT FOR SOFTWARE OF Arachnoid Biometrics Identification Group Corp.
Software: 1 each
This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and the mentioned author of this Software for the software product identified above, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not install or use the SOFTWARE PRODUCT.
SOFTWARE PRODUCT LICENSE
Copyright laws and international copyright treaties, as well as other intellectual property laws and treaties protect the SOFTWARE PRODUCT. The SOFTWARE PRODUCT is licensed, not sold.
1. GRANT OF LICENSE.
Accept
Reject
Back
Next
Cancel

3. Enter Serial Number, Click “Next” to continue.

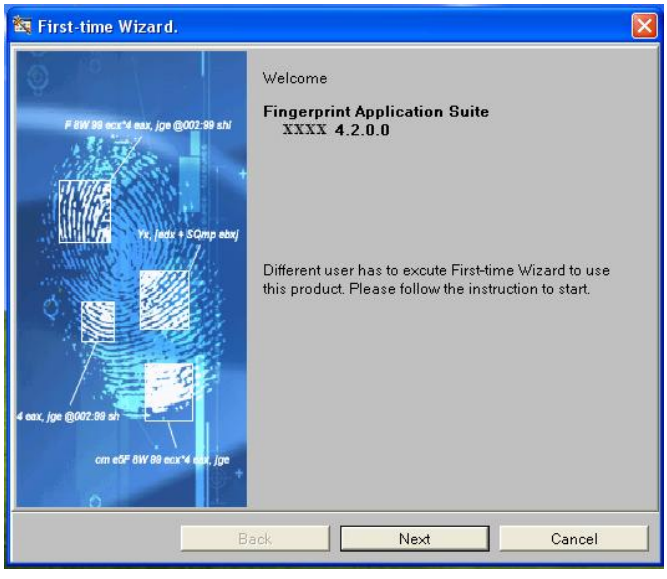


4. Select destination folder for the application. Default path is “C:\Program File\Fingerprint Application\XXXXX”. (“XXXXX” represents product model number)

You can also change destination folder. To do, click “Browse” to selection desire installation path.



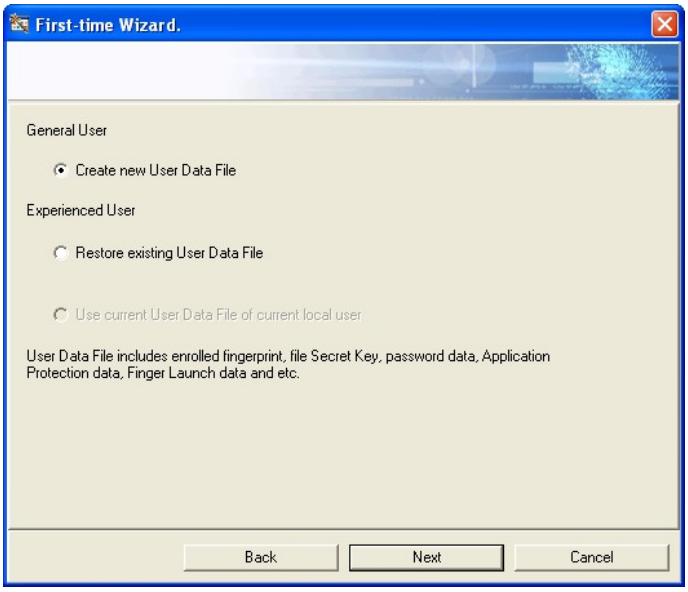
5. After selection of destination folder, the next step is to execute “First-time Wizard” to enter “First-time Wizard” welcome screen.



Note

Users of different accounts will have to execute “First-time Wizard” individually to use this product’s full feature.

6. This step is separated into “General User” and “Experienced User”. For first-time user, it is recommended to select “General User”. For those that has used this software before, you can select “Experienced User”.

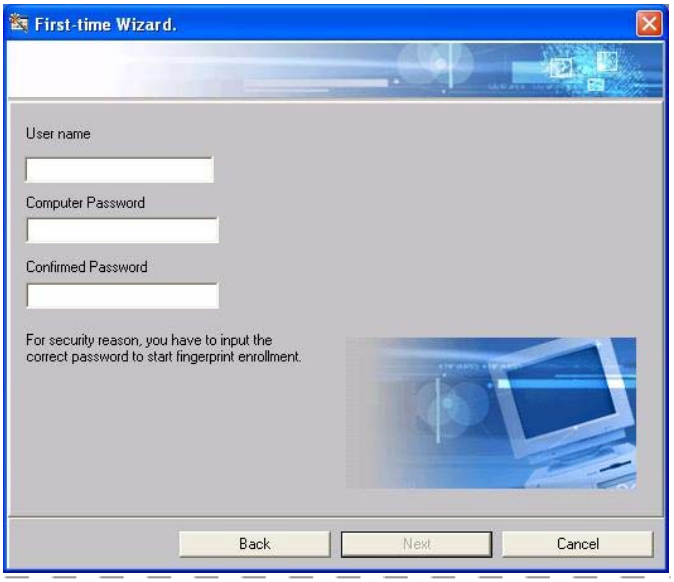

First-time Wizard.
General User
Create new User Data File
Experienced User
Restore existing User Data File
Use current User Data File of current local user
User Data File includes enrolled fingerprint, file Secret Key, password data, Application Protection data, Finger Launch data and etc.
Back
Next
Cancel

General User: To generate new User Data File

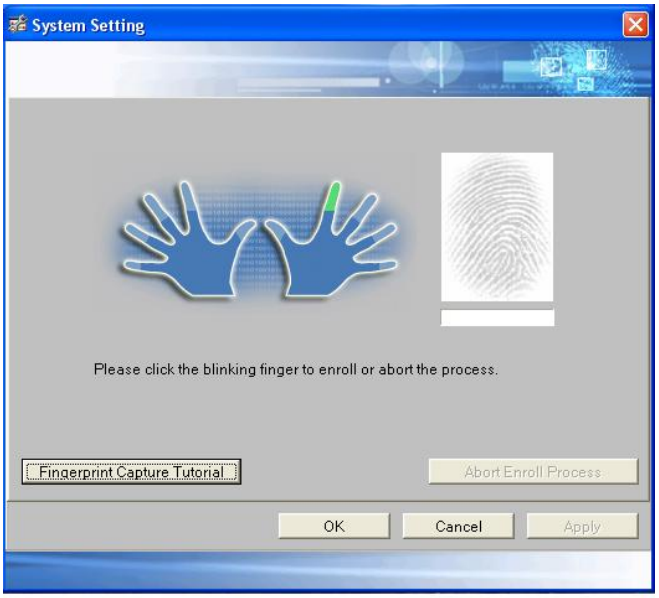
Experienced User: There are two categories, one is for those that will use previously backed-up User Data File, the other one will use current User Data File.

The difference between the two categories is that the first category user can select to restore User Data File, the second category user will load User Data File that was not remove when uninstalling previously installed application (please refer to “What is User Data File” and “Uninstall Application” of this manual”

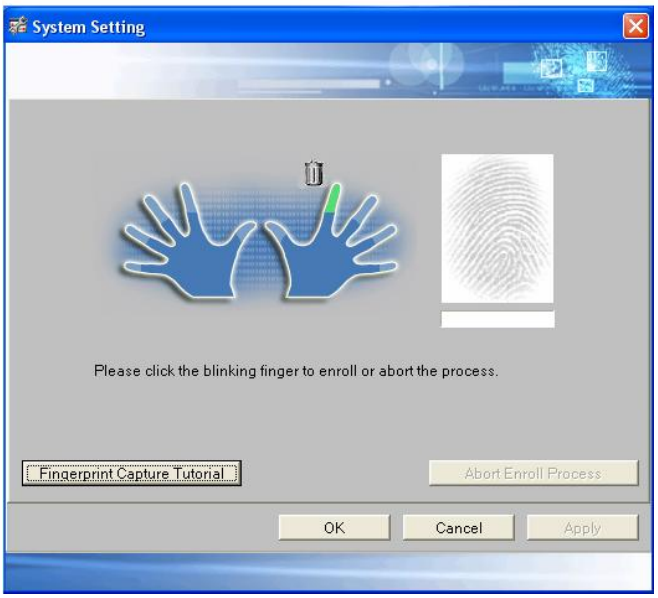
7. Please enter user computer login password in appropriate files (due to security reason, please make sure your compute account password is not blank). Entering password that does not match the password used for login in the system will not start fingerprint enrollment.



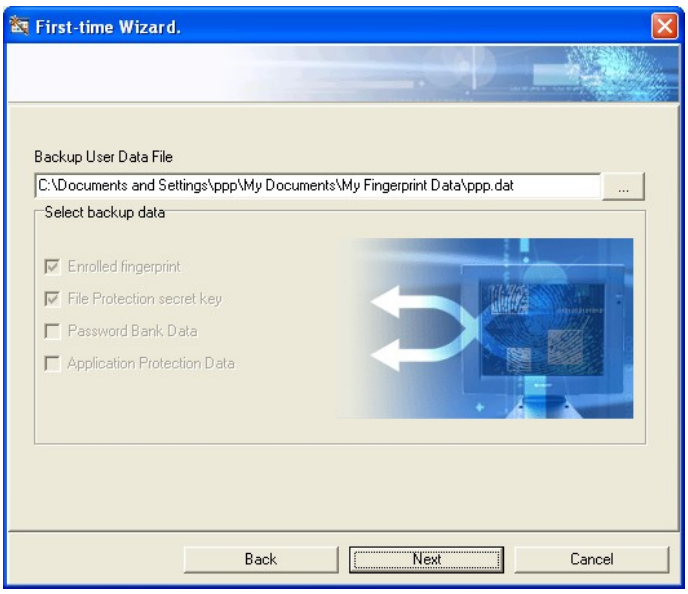
8. Select finger that is blue and blinking to proceed with fingerprint enrollment, then follow instruction to input fingerprint (Please refer to “Instruction on Fingerprint Input” section of this manual on input method). You may continue fingerprint enrollment until all ten fingers are enrolled.



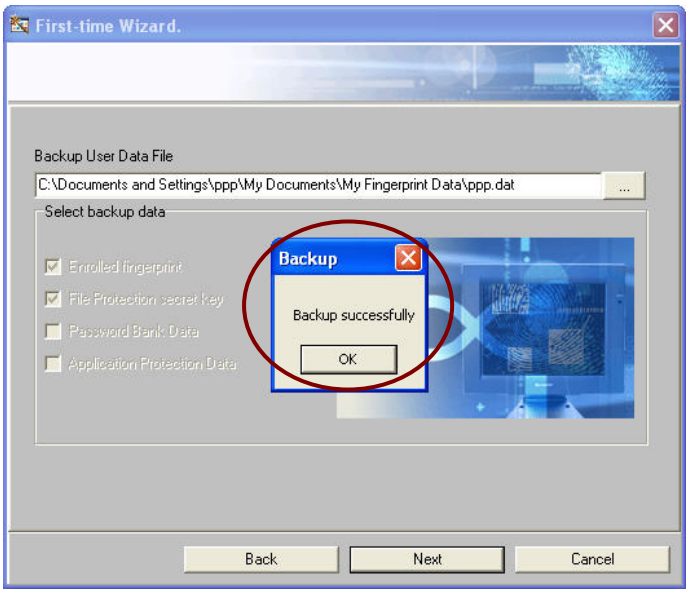
When installing this fingerprint application, user has to enroll personal fingerprint data. The fingerprint data will be used as passport for this application. You may remove or add fingerprint again through “System Setting” (please refer to “System Setting” of this manual)



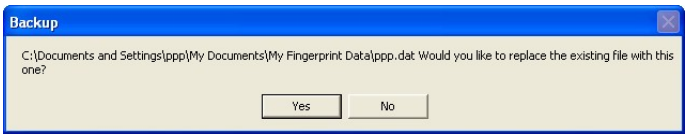
9. This step will back up your fingerprint data and file encryption key (please refer to “Overview” for explanation on key). You may save the backup file (*.dat) to default path of this application (C:\Documents and Settings\Administrator\My Documents\My Fingerprint) or you may click “Browse” to selection another path. Click “Next” to save the data.



Click “OK” after “Backup successful” dialog box shows up to proceed to next step.

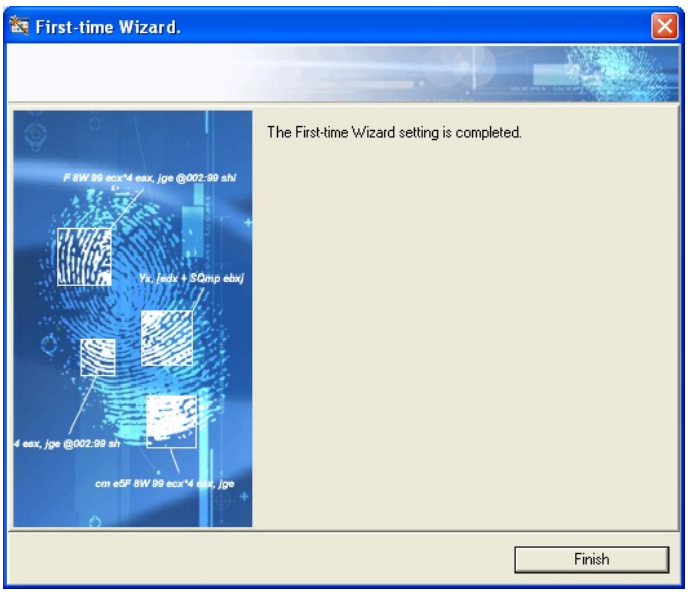


If backup folder has a file with the same file name, a warning dialog box will appear.

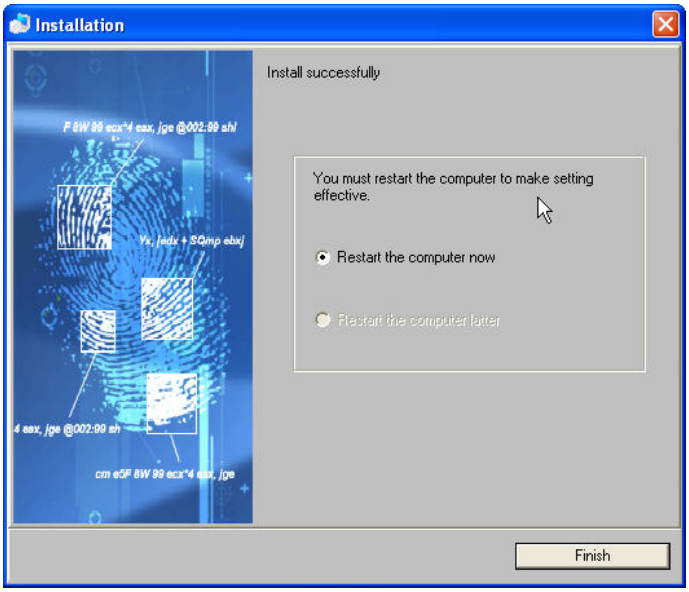

Backup
C:\Documents and Settings\ppp\My Documents\My Fingerprint Data\ppp.dat Would you like to replace the existing file with this one?
Yes
No

Reason to backup User Data File: When you have to reinstall this application, restoring backup file will eliminate the need to build fingerprint again, and it will allow you to open originally protected files.

10. Complete “First-time Wizard” setup, click “Finish” to continue following steps.



11. After installation, this application will automatically restart computer.



Uninstall Application

You can follow below procedure to uninstall this application

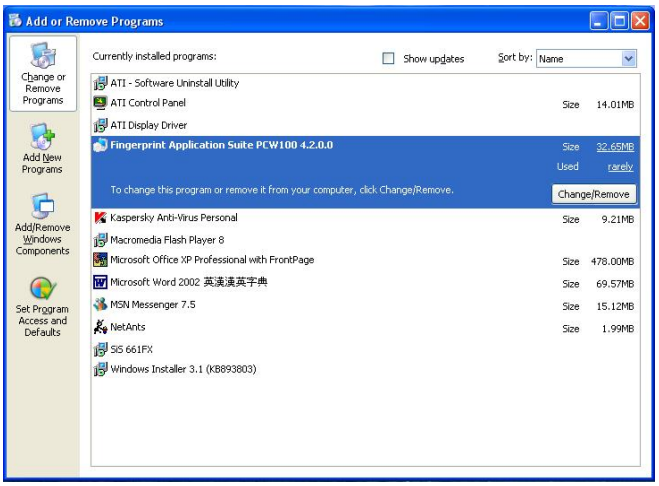
Operating procedures

1. You may uninstall application from three places.

a. From “Start/All Programs/Fingerprint Application/XXXXX/System/Uninstall” (“XXXXX” represent product model)

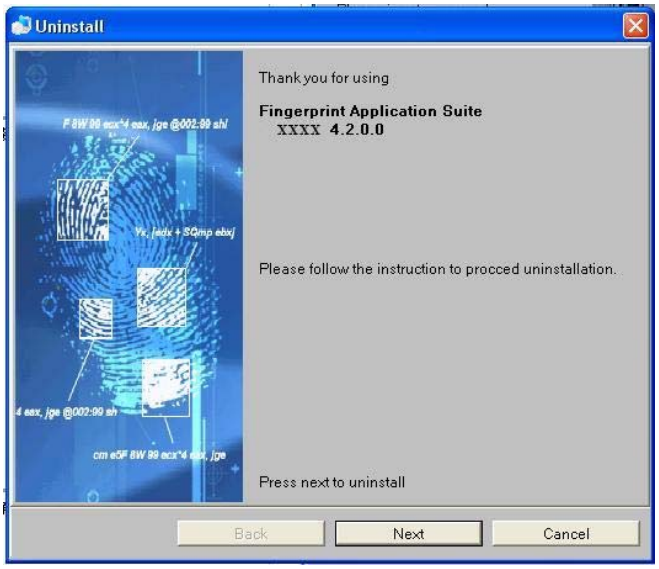
b. Right click on short-cut icon located on toolbar, then select “System/Uninstall” to remove this application.

c. Go to Control Panel “Add or remove programs”, select XXXXX to remove (This figure is based on Windows® XP UI), then follow computer instructions to complete removal. (“XXXXX” represent product model)



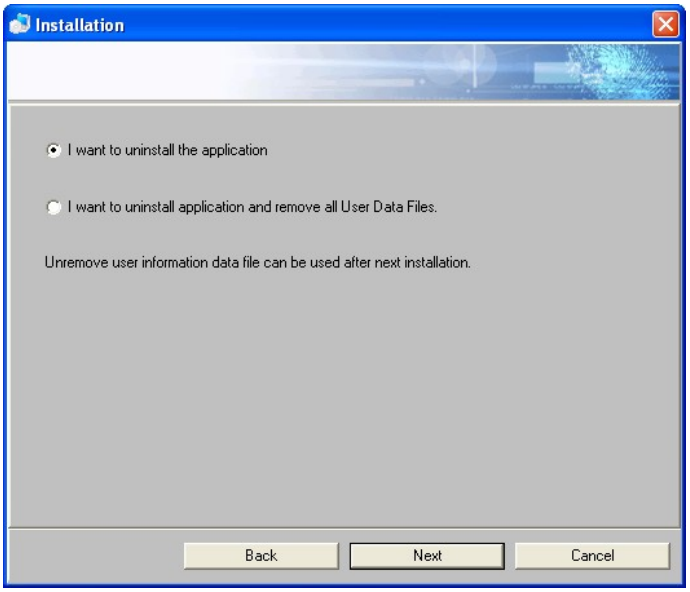
2. Before removing application, identity will need to be confirmed. Please input fingerprint or user password. Application will be removed after confirmation.

3. Entering uninstall page. (“XXXXX” in figure represents product model)



4. This step has two selections: “I want to uninstall the application” and “I want to uninstall application and remove all User Data Files”.

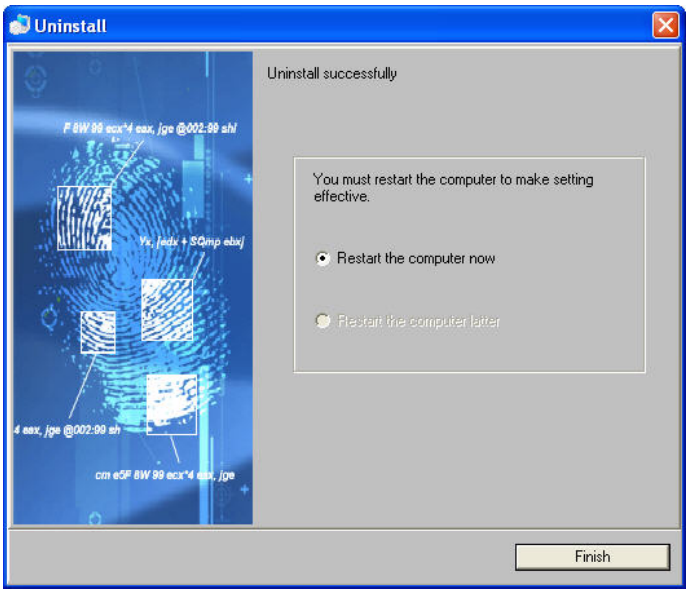
I want to uninstall the application: Only remove the application. Previous User Data Files will be saved. Next time when you login with the same account and reinstall, you can select “I want to use current User Data Files” to continue use previous User Data Files in next installation. (Please refer to “Installation method” of this manual)


Installation
I want to uninstall the application
I want to uninstall application and remove all User Data Files.
Unremove user information data file can be used after next installation.
Back
Next
Cancel

I want to uninstall application and remove all User Data Files: Remove application and User Data Files. Unless original User Data Files are restored, it is not possible to open, edit previously protected files.

> Note
> Before uninstalling application, please backup User Data Files to prevent situations where it is not possible to access previously protected files.

5. Computer will restart automatically after application is uninstalled.



Operating Instructions

To Start Using

Operating procedures

1. After installation is completed (including execution of First-time Wizard) and the computer has restarted, you will be able to use this application. We will show you operating instructions for System Setting, Backup, Restore, Password Bank, File Protection, Application Protection, Finger Launch, Search for Protected Files and Hide/Display icon on toolbar etc.

> Note
> If you are not the same person who installed the program (different login account), please execute “First-time Wizard” to register fingerprint before using the application. (please refer to “Installing application ” step 5 to step 10 of this manual)

System Setting

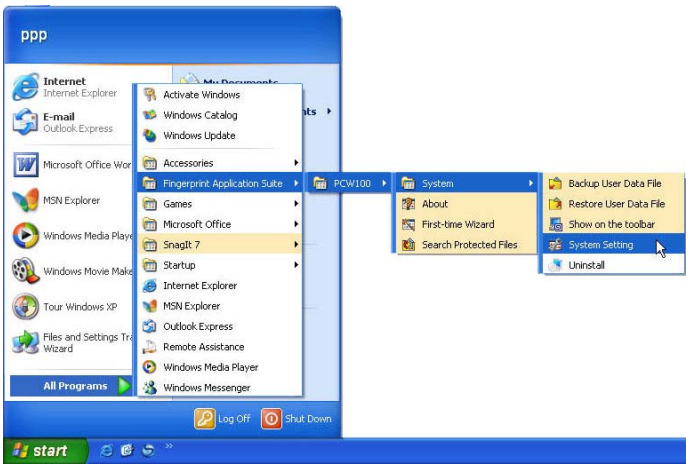
System Setting includes: Fingerprint Management, General Setting, Computer Protection Management, Finger Launch, Password Bank Management, Application Protection Management.

Operating procedures

1. You can execute “System Setting” from two locations:

a. From “Start/All programs/Fingerprint Application/XXXXX/System/System Setting” to execute this function. (“XXXXX” represent product model)

b. Right click on short-cut icon located on toolbar, then select “System/System Setting” to execute this function.



Fingerprint Management

You can enroll new fingerprint data or delete it from this page.

Fingerprint Enrollment

Operating procedures

1. Please select blinking finger to enroll, then follow instruction to input fingerprint (please refer to “Instruction on Fingerprint Input” of this manual). When best quality fingerprint are captured, fingerprint enrollment is completed.

You may continue to enroll fingerprint enrollments for all ten fingers.

Delete Enrolled Fingerprints

Operating procedures

1. Please move cursor on top of gray finger that is intended for deletion. At this time, cursor will become , click on that finger will remove that fingerprint. You may continue to remove fingerprints, but you have to save at least one fingerprint.

Note

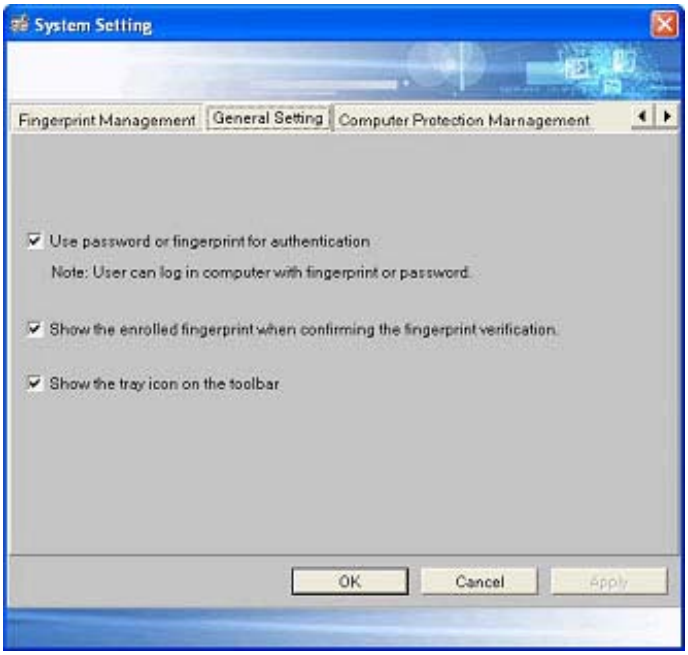
For the safety of your computer, this application requires that at least one fingerprint file is

General Setting

Configurations on this page includes: Use password for authentication, show the enrolled fingerprint when confirming the fingerprint verification, and show tray icon on toolbar.

Operating procedures

1. Meaning of each item appears on this page is explained below:


System Setting
Fingerprint Management
General Setting
Computer Protection Management
Use password or fingerprint for authentication
Note: User can log in computer with fingerprint or password.
Show the enrolled fingerprint when confirming the fingerprint verification.
Show the tray icon on the toolbar
OK
Cancel
Apply

User password for authentication: Other than enrolled fingerprints, is computer account password allowed to use for identity confirmation?

This setting does not include login identity confirmation when turning on computer. When login to computer, identity can be confirmed using either fingerprint or password whether it is checked or not checked.

Show the enrolled fingerprint when confirming the fingerprint verification: whether to remind user of which fingers are enrolled on identity confirmation UI. This reminder will appear on upper right corner of UI. Green finger represent the finger is enrolled.

Show tray icon on toolbar: whether to show tray icon on button right corner notification area. System default is set to show.

Note

If “Use password for authentication” is not allowed, then only fingerprint can be used for authentication. Authentication cannot be done using computer account password, this implies that password entry are is gray out

Computer Protection Management

Computer protection function will prevent others from using your computer when you are away from your computer. There are three ways to protect your computer: login computer, lock computer, screen saver. For detailed usage, please refer to “Computer Protection” of this manual.

Operating procedures

1. Please input your computer login password in the “Computer Password” box. To make sure the password is correct, please input r the same password in “Confirmed Password” box as you inputted in the previous box. If the password is different from the password that login to computer, the setting of Computer Protection will not continue.

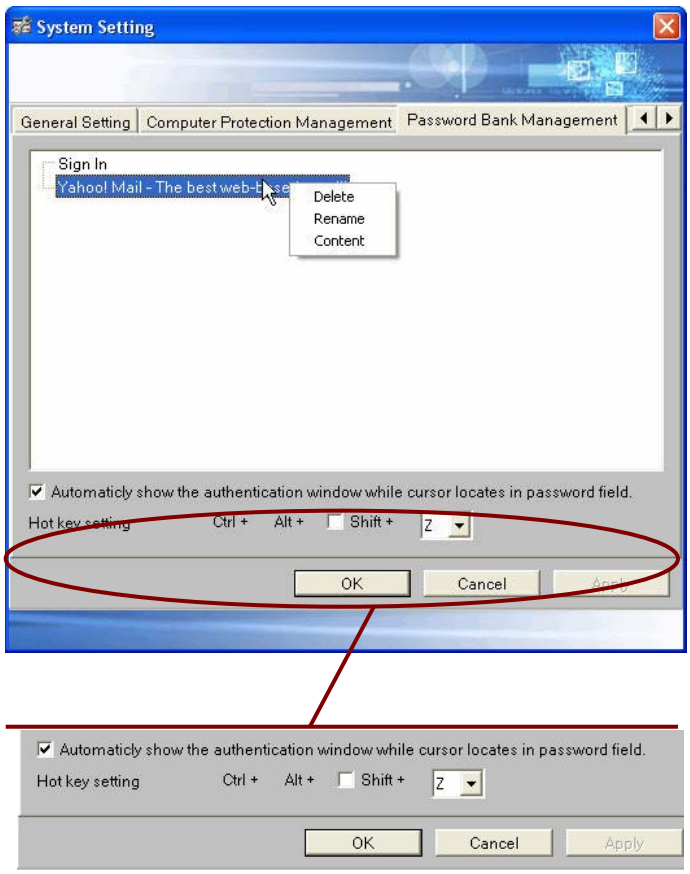
Password Bank Management

This page is able to manage password bank data and modify password bank hotkey setting. For usage of “Password Bank” and methods on how to save account, password, please refer to “Password Bank” of this manual.

Operating procedures

1. Manage Password Bank: You can delete, rename and edit password bank. Right click on the desired management item to select to execute one of the above functions. Select “Edit” to edit the account and password of the item.

Modify password bank hotkey setting: Set hotkey to remember applications or website account and password. Currently, hotkey is set to “Ctrl+Alt+Z”, you may change to other hotkey that you are familiar with.



Application Protection Management

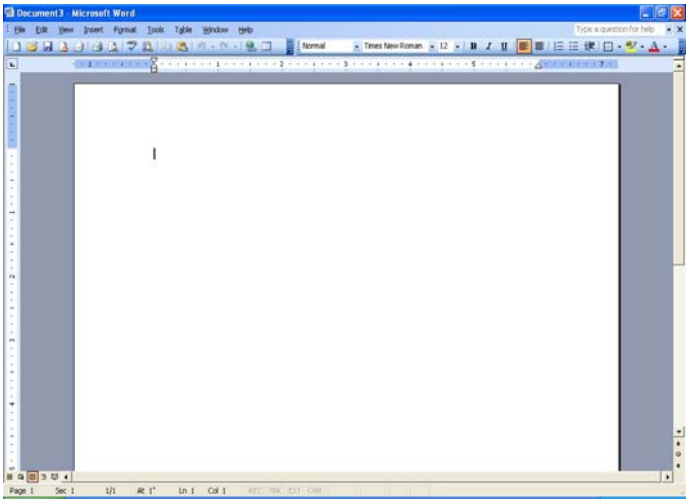
Protect applications that you do not want others to run. For “Application Protection” usage please refer to “Application Protection” in this manual

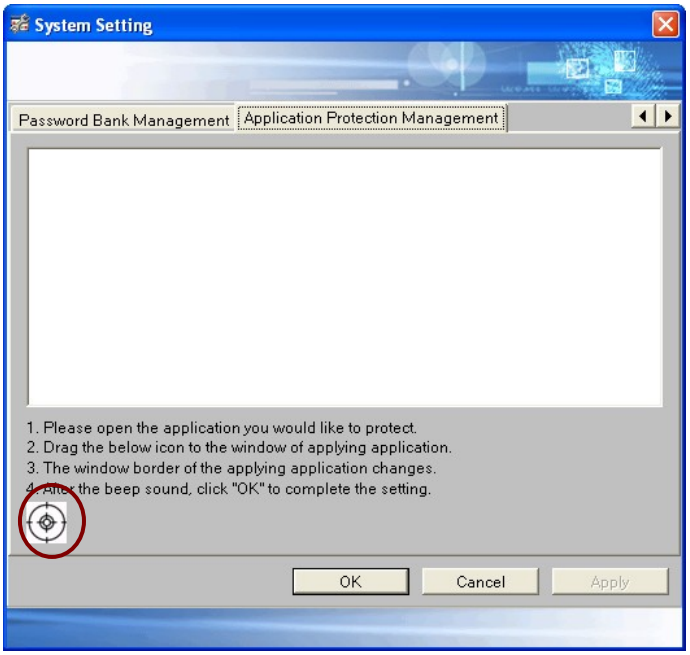
How to setup Application Protection

Operating procedures

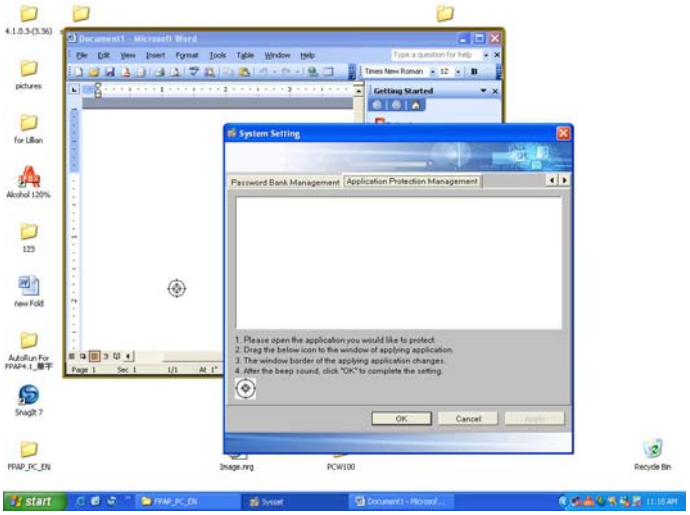
1. Please open the application that you would like to protect (we use Microsoft® Word as an example here)

Move cursor to top of icon located at lower left corner of the UI




System Setting
Password Bank Management
Application Protection Management
1. Please open the application you would like to protect.
2. Drag the below icon to the window of applying application.
3. The window border of the applying application changes.
4. After the beep sound, click "OK" to complete the setting.
OK
Cancel
Apply

2. Drag the icon to the window of the applying application, the window border of the applying application changes.


System Setting
Password Bank Management
Application Protection Management
1. Please open the application you would like to protect.
2. Drag the below icon to the window of applying application.
3. The window border of the applying application changes.
4. After the beep sound, click "OK" to complete the setting.
OK
Cancel

3. Release the mouse and a beep sound will be played. Protection setting is complete when confirmation dialog box shows up.

Terminate Application Protection Management

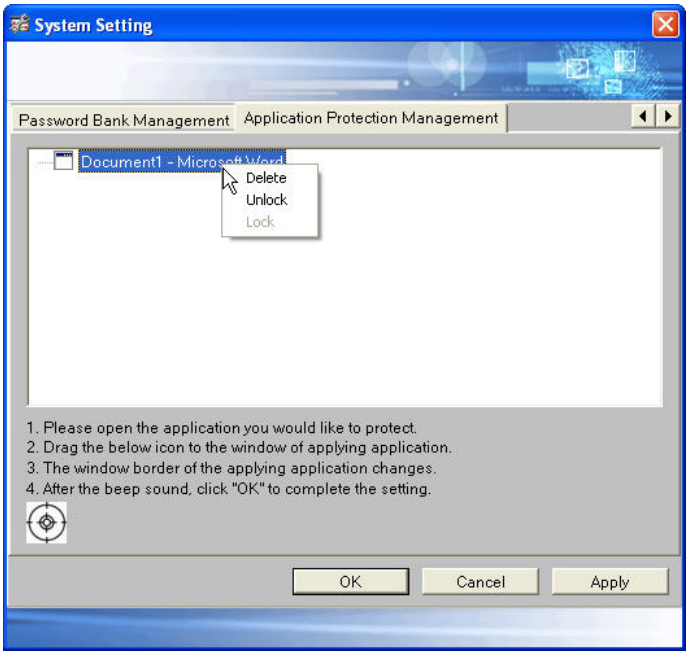
Operating procedures

1. Right click on the application that you intend to apply management function.

Terminate Protection: Terminating application protection (The application remains in the list)

Configure protection: Protects those applications that have terminated their protection in the list.

Delete: Delete application. The application will be removed from the list and protection on the application will be terminated.

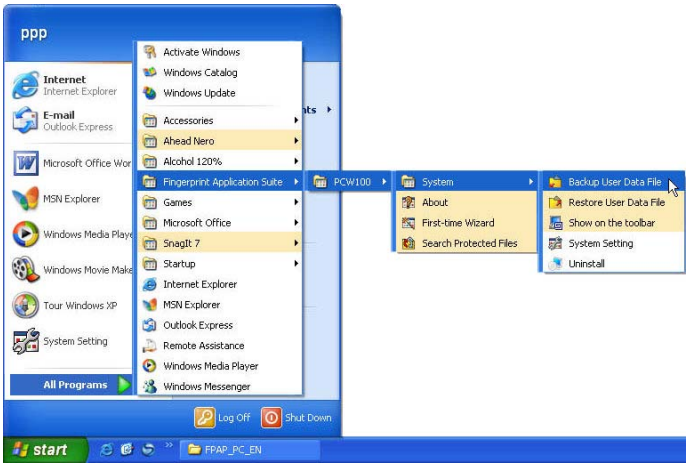

System Setting
Password Bank Management
Application Protection Management
Document1 - Microsoft Word
Delete
Unlock
Lock
1. Please open the application you would like to protect.
2. Drag the below icon to the window of applying application.
3. The window border of the applying application changes.
4. After the beep sound, click "OK" to complete the setting.
OK
Cancel
Apply

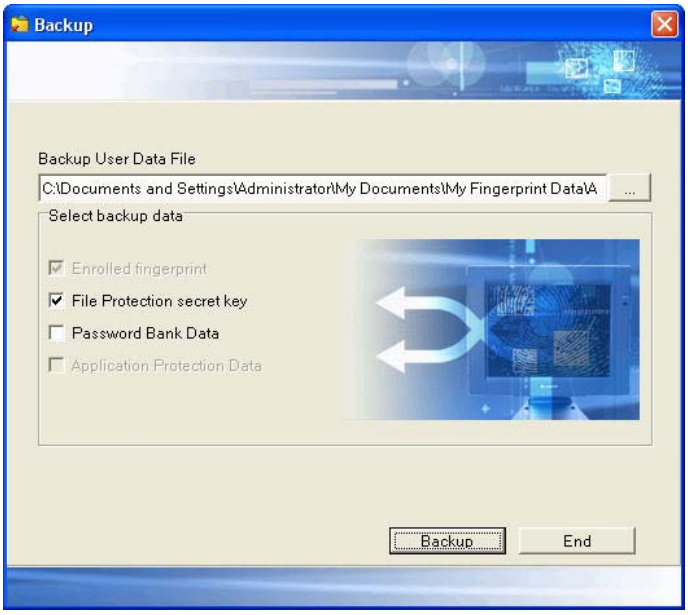
Backup

Backup User Data Files you have set up. Purpose of backup User Data Files: When you have to reinstall this application, restore backups will eliminate the need to enroll fingerprints again and it allows you to access originally protected files.

Operating procedures

1. Specify location to back up files. Backup files should at least include enrolled fingerprint files, other exporting items are optional. Click “Backup” after you have confirmed on selections.





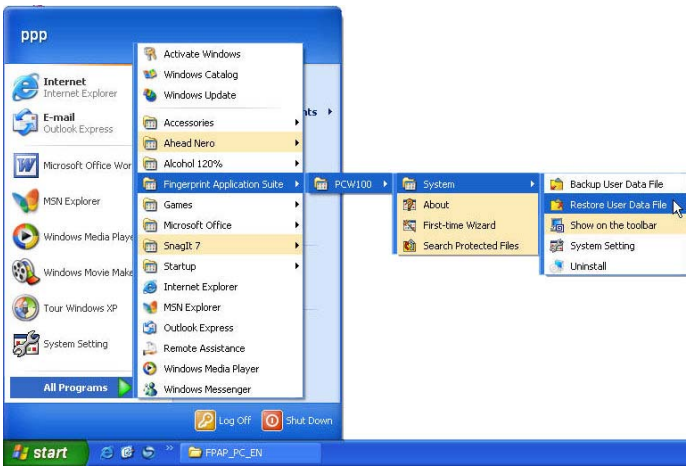
Restore

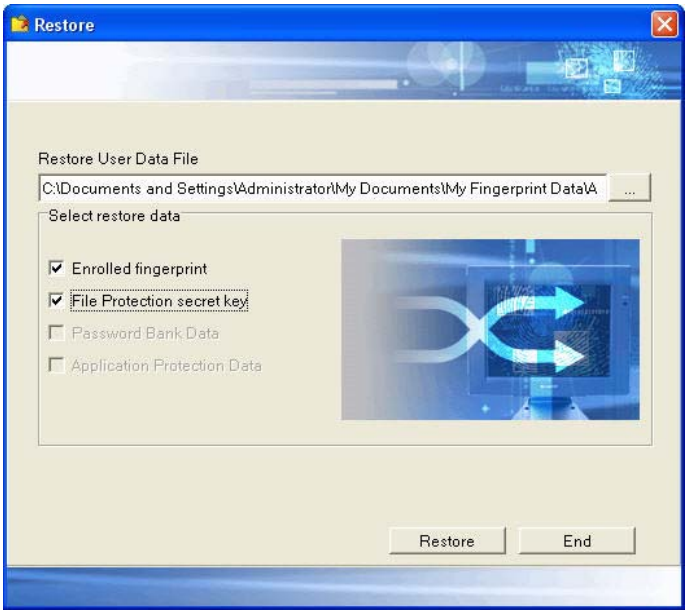
To Restore User Data Files you have backed up previously. Restoring backups will eliminate the need to enroll fingerprints again and it allows you to access originally protected files.

Operating procedures

1. Restore data item will only allow selection of data items included in backed up files.

Select path to backed up file, then select the backed up file. Please select data items you intent to restore from the lower part of the interface. Click “Restore” to successfully restore data.





Password Bank

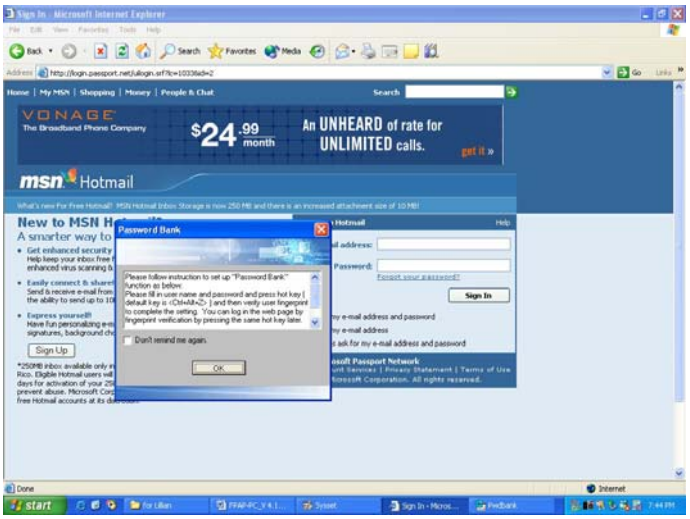
To record the homepage and the application user account and password（Below instructions take the operation procedure of the homepage and the network disk driver as the example）

Password Bank Management

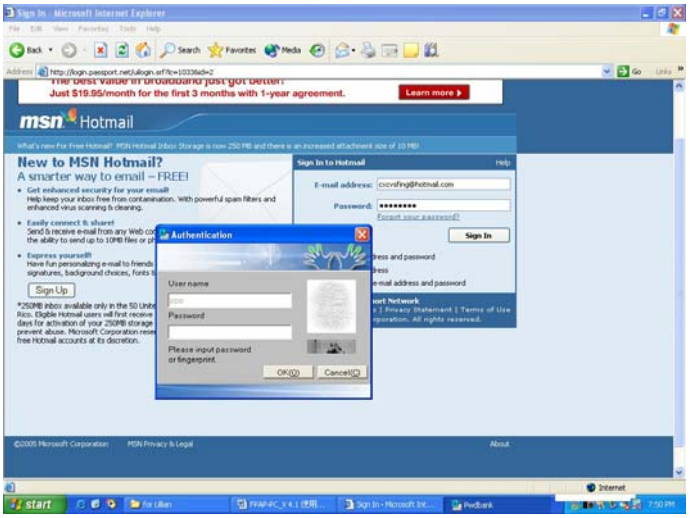
Manage password bank on the homepage

Operation procedure

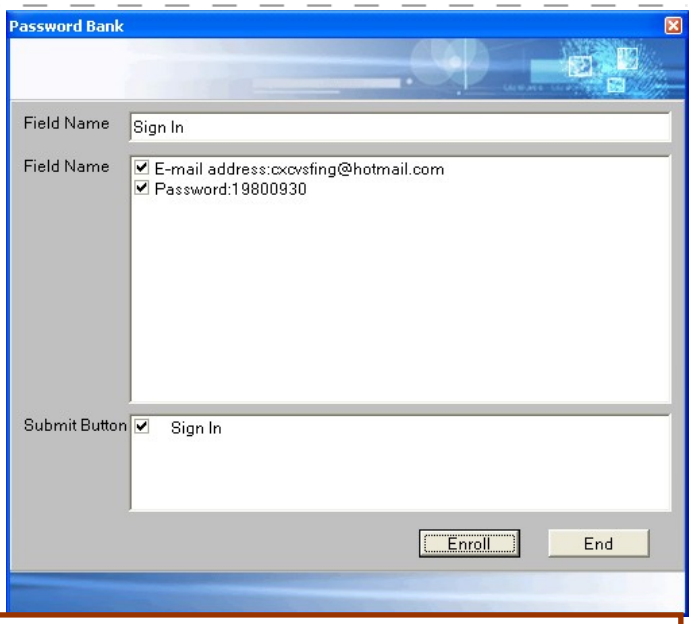
1. When move the cursor to the password entry location of the homepage, a reminder dialog box will automatically pop out , you can follow the instruction of the reminder dialog box to save login account and password.



2. Press the submit button after fill in the correct user account, the password in the password and the authentication fields, then an identification authentication window will appear, and user can sign in after the authentication is confirmed。



3 After the user account has been confirm will to pop up following constructs picture: The user may choose the preserved items voluntarily.（Please to the mouse clicks onto the check box in front of items to check off or not.）。



注意

1.The possible some softwares or websites are not to support this function。

2 Yoy will be allowed to choose "No longer to remind me" to let the next time not be able to appear the remind Windows.

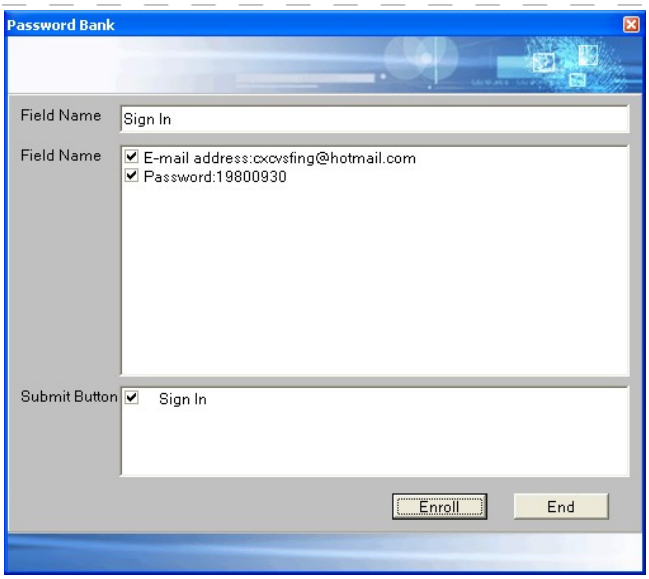
Other password bank management

Some software possibly does not support this function, please use the hot key to manage the password bank.（Below instructions take the operation procedure of the network disk driver as the example）Operation procedure

1.Fill in correct user name and password then press hot key (default key is “Ctrl+Alt+Z”.. You can setup your
customized hot key. Please refer to “Password Bank Management” section for hot key set up), an identification authentication window will appear.

Map Network Drive
Connect As...
By default, you will connect to the network folder as TITAN\titan.lee. To connect as another user, enter their user name and password below.
User name:
titan
Browse...
Password:
OK
Cancel
Connect using a different user name.
Sign up for online storage or connect to a network server.
< Back
Finish
Cancel

2. After the authentication is confirmed, below setup screen will appear. The user may choose the items that user would like to save.. （use mouse to check or
uncheck box in front of each item to select or unselect .）



3. When enter the same webpage, only input the user name and press the hot key, after it is confirmed, then you can log in.

注意

The system can recognize the user and password of different destination, When destination has been changed, The user possibly must record account and the password again.

Usages for Password Bank

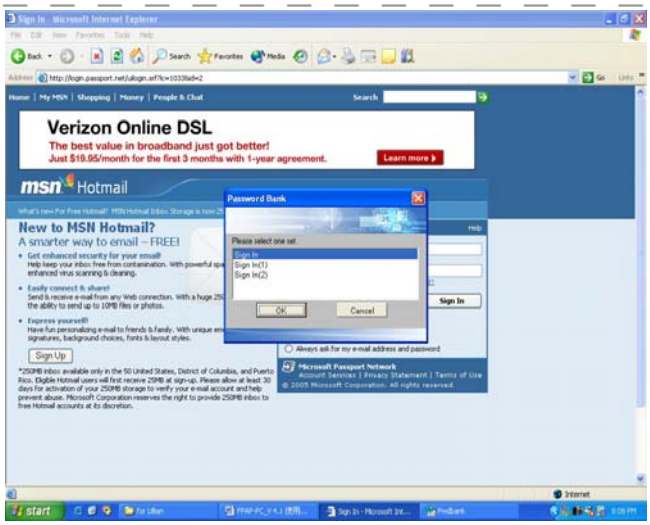
Operation procedure

1. When move the cursor to the password entry, an identity authentication window will pop out. When press the "Yes" button, the recorded user account and the password will be applied to login. When press "No" button, other user account and the password can be applied to login.（If you want to store other user accounts, please press "No" button, and repeat the operation procedure of the Password Bank.）

Password Bank
You have registered ID/Password for this page. Do you want to fill them automatically by fingerprint? Otherwise you may choose [No] to register another ID/Password.
Yes
No

2. After presses down the "Yes" option, can automatically spring up the confirmation Windows, after the authentication confirmed, then automatically leads the stored user account and the password to sign in。

3. When in the same page has comprehended more than two user accounts and the passwords, When the vernier puts in the password field, will first spring up the list of stored password bank, After chose the user account, then carries on the status confirmation。


Verizon Online DSL
The best value in broadband just got better!
msn Hotmail
New to MSN Hotmail?
A smarter way to email – FREE!
Password Bank
Sign Up

File Protection

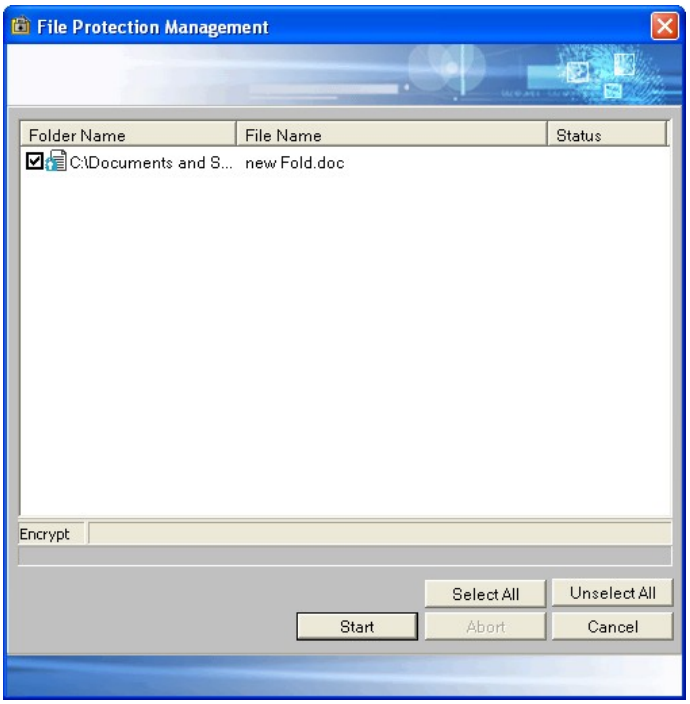
This chapter includes: file encryption, decryption, folder encryption/decryption and editing encrypted documents. You can proceed with File Protection regardless if you are on desk top or file manager. (Below introductions uses files on desk top as examples)

File Encryption

Operating procedures

1. Using files on desk top as examples. Right click on the file intended to encrypt, an identity authentication window will pop up.

2. Check the file that you intend to encrypt that is listed in “File Protection Management” window. Click “Start” to proceed with file encryption. After it is done, file short-cut icon will be shown as under encrypted state.



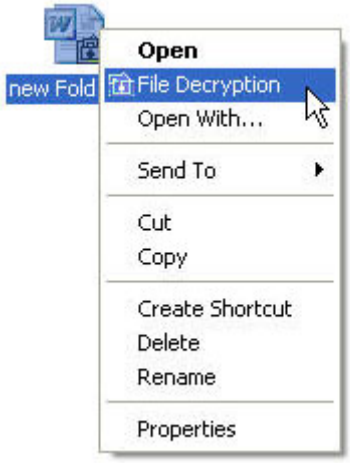
Note

Right-click on a folder and select “file protection” or “disable file protection”, user could perform enable or disable file protection directly.

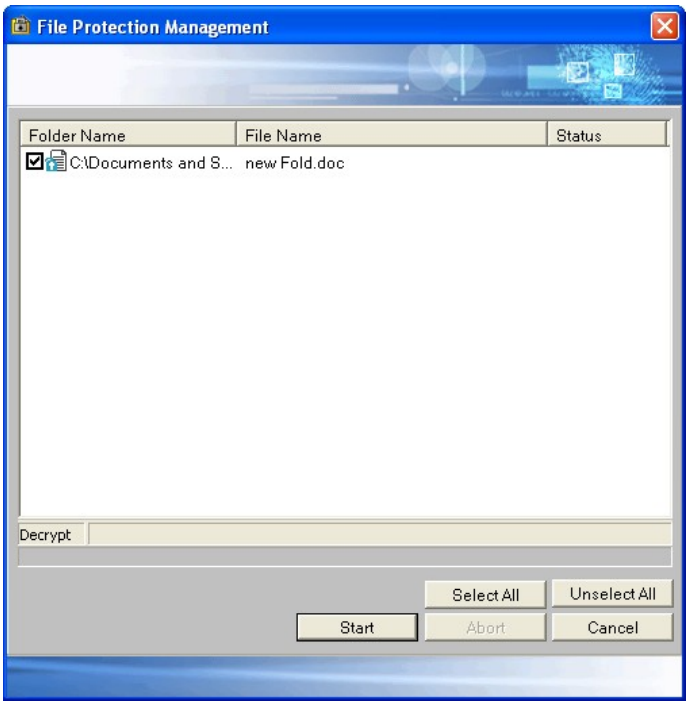
File Decryption

Operating procedures

1. Right click on file that is encrypted and select “File Decryption”. After identity is authenticated, the file will be decrypted.



2. “File Protection Management” will pop up, check the file intended to encrypt, then click “Start” to start encryption. After it is done, file short-cut icon will be shown as under encrypted state.



Editing Encrypted Files

Operating procedures

1. Please decrypt the files before editing the protected files.

Computer Protection

Computer protection can avoid others from using your computer without permission when you login your computer or when you are away from your computer. There are three ways to protect computer: Login computer, locking computer, screen saver.

Login Computer

Operating procedures

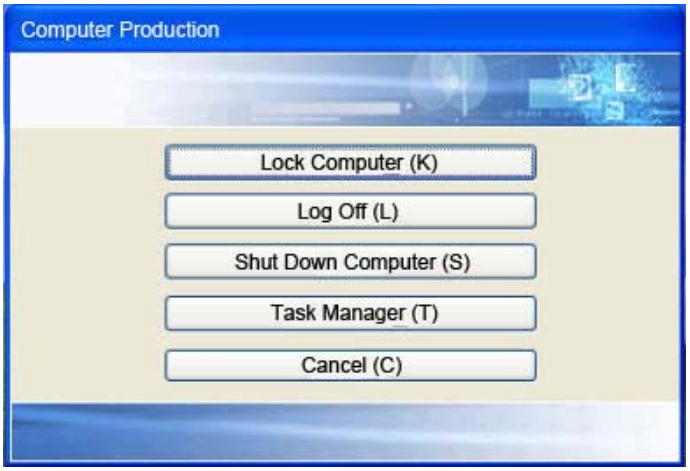
1. Before user can start computer, user has to authenticate user's identity. Please input fingerprint using fingerprint product or key in user name and password. Only after identity is authenticated can user login to computer.

Locking Computer

When you have to temporarily leave your computer, to avoid others from using your computer without permission, this feature can lock up your computer.

Operating procedures

1. Press Ctrl+Alt+Del keys together. “Computer Protection” window will appear (refer to figure on right). Press “Locking Computer” to lock up your computer.



Below feature is a Windows® build-in feature. A brief introduction follows:

Log Off: Log off current user’s account for another user to login.
Shut Down Computer: turning off computer

Task Manager: Examine or end tasks currently running in computer.

Cancel: If choose not to do anything, choose this to leave this window.

2. Locking computer window is shown on right. If you want to continue to use the computer, your identity must be authenticated to unlock the computer and continue usage.

> Note
> PC protection function needs a reboot to take effect.

Screen Saver

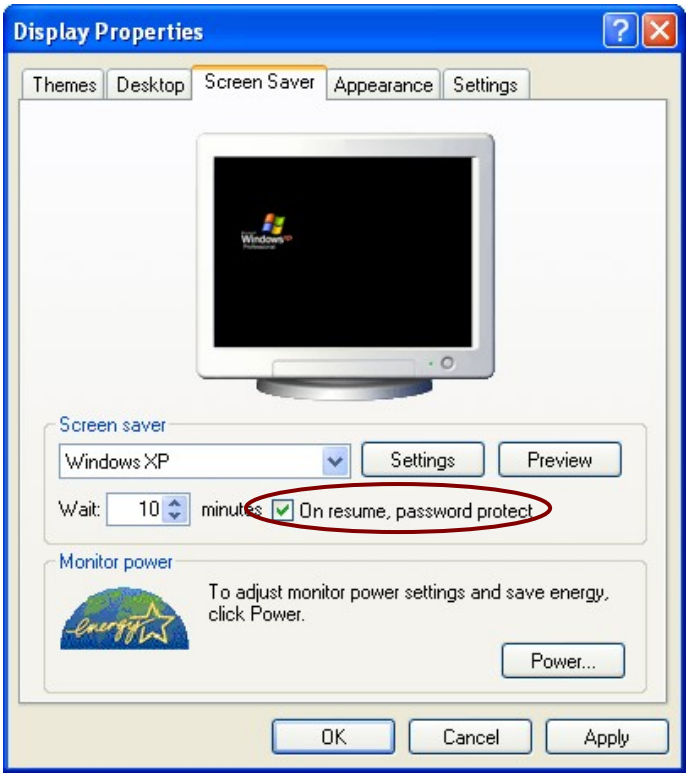
After screen saver, proceed with identity authentication to make sure that your computer will not be used by others without permission.

Set up Screen Saver

Operating procedures

1. To set up screen saver, go to “Control Panel/Display/Screen Saver” (or right click on desk top, select “Properties/Screen Saver”).

Please check “password protect” to enable identity authentication function.



Usages of Screen Saver

Operating procedures

1. When you touch your computer after screen saver is running, you will be asked to authenticate yourself. After your identity authenticated, computer's last state before screen saver will resume so you can continue to use the computer.

Application Protection

Operating procedures

1. Please complete Application Protection set up (please refer to "Application Protection Management" in this manual). When you want to execute protected application, you will be asked to authenticate your identity before you are allowed to execute the application.

Search Protected Files

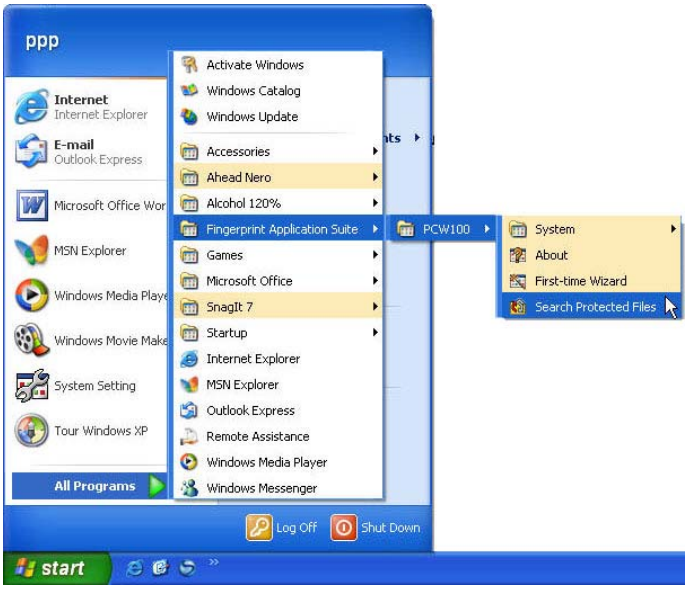
This function can search for all protected files in the computer.

Operating procedures

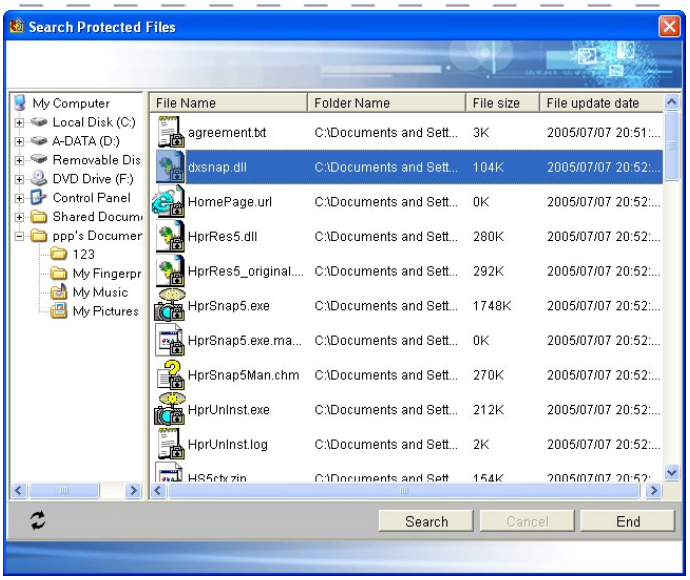
1. You can execute “Search Protected Files” from two locations:

a. From “Start/All programs/Fingerprint Application/XXXXX/ Search Protected Files” to execute this function. (“XXXXX” represent product model)

b. You can right click on the short-cut icon located at tool bar, then select “Search Protected Files” to execute this function.

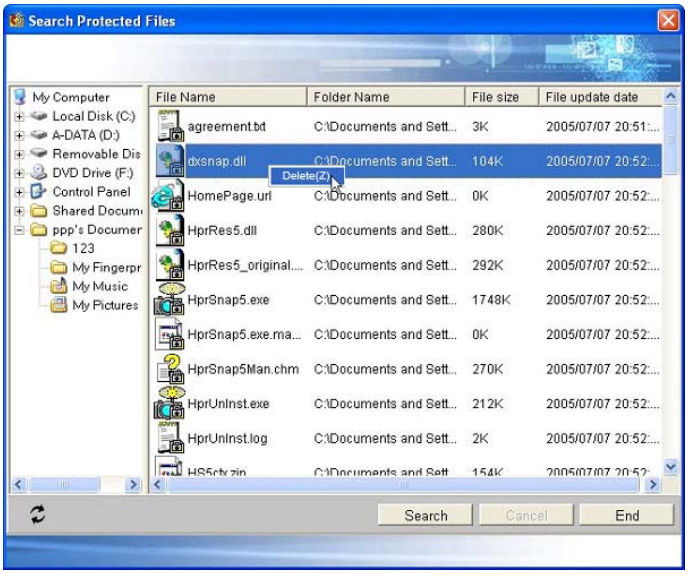


2. You can use this function to search for protected files: First, select the drive to search from left side, then click “Search” to start searching. (For instruction on how to protect file, please refer to “File Protection” in this manual)



3. After getting the name and the path to protected file, right click will delete this protected file.

Use mouth to click file that can be opened (identity must be authenticated first), to start search again, please select a drive then click search, to close please click “Finish”.



Hiding/Displaying icon on toolbar

Hiding or displaying icon on toolbar.

Operating procedures

1. You can execute this function from three places:

a. From “Start/All Programs/Fingerprint Application/XXXXX/System/Show on the toolbar” to execute this function (“XXXXX” represents product model)

b. Right click the short-cut icon on toolbar, select “System/Hide from the toolbar” to execute this function

c. Regular set up UI of system set up

> Note
> If you have already hidden the icon, you can display the icon on toolbar again using following path: from “Start/All Programs/Fingerprint Application/XXXXX/System/Show on the toolbar” to execute this function. (“XXXXX” represents product model)

FAQ

1. Why does fingerprint enrollment fail?

Answer: Every time a fingerprint is inputted, it is calculated to get this fingerprint's special characteristics, These special characteristics are cross compared and calculated to produce new, better quality fingerprint characteristics. When this is amounted to certain level, the enrollment is then completed. This is to ensure security.

2. Is it possible to make sure that encrypted file will not be deleted?

Answer: Files encrypted with fingerprint is to ensure that file's legal and authorized usage. Its content can only be read or edited by user that has passed fingerprint authentication. Any other user will not be able to delete the encrypted file.

3. Why can't I open encrypted file with fingerprints that are enrolled?

Answer: This is possible when the quality of fingerprint characteristics was poor when processing fingerprint enrollment. All of these may affect the result of fingerprint authentication. Therefore, it is strongly recommended that user enroll two or above fingerprints. When one fingerprint suffers from above situations, there is another fingerprint that can be used for authentication.

4. Why are these sub file names of *.exe, *.ini, or *.dll, which can't be executed the function of file protection?

Answer: The AP can't be worked properly by these kinds of files, therefore, the AP will restrain the function to prevent it occurs. If you intent to protect the *.exe files, you may execute the "Application Protection" function to complete it.

5. Why can't I use my password to verify my identity when accessing my user data file?

Answer: Because your user data file contains confidential data, you can only access your user data file with fingerprint verification. This better protects your personal data and prevents access by non-authorized persons.

6. Why some files under folders such as C:\Windows cannot proceed with file protection.

Answer: Because folders like C:\Windows usually contains system files and could cause abnormality of other programs. Therefore, we will disable the file protection function under C:\Windows, C:\Program Files, C:\ and D:\ etc…

7. Why I am not prompted with enrolled finger when in a Windows logon screen?

Answer: Because the fingerprint software supports multi-user. Therefore user won't get prompted with enrolled finger in a Windows logon screen.

8. Why is that after storing the user backup data, but the fingerprint quantities in the enrolled file is more than the original file?

Answer: To avoid any possibilities be occurred, after changing the user enrolled data, the AP will execute the "Appending" function to backup your fingerprints automatically. In other words, after enrolling your right index fingerprint, you will not read it in the backup file, but will find it in the stored backup file.

9. Why can't I see "Decrypted files" function once I click the mouse right key on the Chinese folder / file name in the English OS?

Answer: This is the OS languages compatibilities issue, Microsoft® Windows also has the same problem, therefore, we suggest you name the folder/file in English to avoid this kind of problems in any languages OS.

Thank you again for using this product!